* NMCI User Awareness Bulletin *

~~~~~~

*** User Action required ***

~~~~~~

EVENT: Telework Improvements, Recommendations, and Best Practices during COVID-19 Pandemic

AUDIENCE: All NMCI REMOTE USERS

DATE/TIME: 17 Mar 2020 - Until Further Notice

SITUATION: To support extended telework requirements during the COVID-19 Pandemic, corrective measures are being implement to best support remote working conditions. Actions include NMCI network changes and sharing practices to enhance the "work from home" environment.

1) When working in an office environment (i.e., NOT teleworking), reboot the workstation/laptop daily and ensure it remains powered on at the end of the workday to allow network changes to occur during the off-hour maintenance schedule. Users DO NOT need to remain logged on; however, machines should remain powered on.

2) Before going home to telework, conduct a workstation reboot and accept the Green Shutdown. This ensures the latest patches and configurations are loaded to the laptop before disconnecting from the NMCI network.

3) CAC reader, mouse, and keyboard for home use. Users must have a Common Access Card (CAC) reader connected to their personal computers to open Outlook Web Access (OWA).

a. As directed by individual commands, users may be authorized to take NMCI CAC readers and peripheral devices from their work locations to support OWA use; however, once a CAC reader is taken home and used in a personal computer, it must remain home. Approval should be coordinated at the local command level. CAC reader specifications are located at: https://dl.cyber.mil/pki-pke/pdf/unclass-dodcac_release1-0_reader_require_v1-01.pdf

4) Laptops are temporarily configured to allow users to connect to a private, secure, Wi-Fi connection at remote locations without establishing a secure connection to the NMCI VPN gateways. This prevents the (5) minute time limit from being enforced and terminating the Wi-Fi connection.

a. Under current conditions and to enhance security users are directed to:

i. Only connect to trustworthy Wi-Fi when required

ii. Disconnect from Wi-Fi when work is complete

iii. Only visit authorized websites while connected
iv. ALWAYS use the secure RAS VPN when using Wi-Fi at a public hotspot

5) If possible, physically connecting the work-laptop to a home cable connection (e.g., Ethernet) is highly encouraged to improve all performance. Many services, such as DCS Web conferencing and training sites, do not require a PulseSecure VPN (uRAS) connection when physically connected to a home network.

6) VPN (uRAS) 2 hour time limit enforced. To ensure a maximum number of users have opportunity to uRAS into the NMCI network, a 2 hour timeout is enforced to disconnect users after 2 hours of operation and allow alternate users opportunity to connect via VPN; users are encouraged to reconnect at earliest opportunity.

7) Outlook Web Access (OWA) will function using any web browser; however, users are only able to download or upload attachments using Internet Explorer (IE) or Edge.
a. The use of IE/Edge for file download and upload provides new, additional flexibility while using OWA and should relieve some of the need for uRAS access.
b. Internal access going from NMCI to OWA should be avoided. If inside NMCI (including uRAS), users are to access Outlook from an NMCI workstation. This reserves OWA access for remote user which is its intended purpose.
c. Additional OWA support can be found at: https://homeport/support/topics/outlook-web-app-(owa)

8) Antivirus Software (AV). Per DoN Telework agreements, users are required to ensure antivirus software is active and up to date on home workstations. Turn on Windows Defender (embedded in Windows 10) to meet the minimum required AV software requirement.

9) JFHQ-DODIN reserves the right to restrict or block streaming media websites (YouTube, Netflix, Pandora, etc.) and may soon block social media websites (Facebook, Instagram, etc.) to maximize operational bandwidth for COVID-19 response.

10) Information Security (IS). When using remote work options, IS remains paramount. While working remote maintain vigilance and adhere to all security protocols. Using personal e-mail and other commercial services (e.g.: Gmail, Zoom, WebEx, and others) for official business is not permitted.

ASSISTANCE: Contact the NMCI Service Desk at 1-866-THE-NMCI (1-866-843-6624) or by e-mail at ServiceDesk_Navy@nmci-isf.com. Refer to the user communication number below.

~~~~~~
~~~~~~~~~

NMCI User Awareness User Bulletin # 20200319 - 0500
~~~~~~
~~~~~~